

Welcome to FT.com, the global source of business news and analysis. Register now to receive 8 free articles per month.

March 19, 2013 2:09 pm

# Hacked PCs falsify billions of ad clicks

By Tim Bradshaw in San Francisco and Emily Steel in New York



One outsourcing company managing others seems risky

Online investigators have exposed a network of hijacked computers that defrauded advertisers by generating billions of fake ad views.

The so-called botnet scheme, which hijacked 120,000 residential PCs in the US and cost advertisers millions of dollars a month, highlights the increasing complexity and opacity of online advertising.

Spider.io, a London-based start-up that tracks web browsing activity, estimates traffic from the “Chameleon” botnet accounted for almost two-thirds of the total visits to certain websites. The inflated number of page views increased advertising revenues for the websites’ owners.

In a report published on Tuesday, Spider.io said the hijacked PCs generated up to 9bn ad views or “impressions” every month across a network of more than 200 sites. Sophisticated software even mimicked cursor movements and mouse clicks, giving the impression that potential consumers were visiting the sites.

“It is difficult to imagine why one would run this type of botnet across a cluster of 202 sites other than to commit display advertising fraud,” Douglas de Jager, Spider.io’s chief executive, said in the report. The websites that attracted the traffic charge an average 69 cents per thousand ad impressions, meaning the botnet is costing advertisers about \$6m a month.

Mr de Jager told the Financial Times that the scheme was just one of many that the online advertising industry had been fooled by – or had chosen to ignore: “We have already identified at

least one other large and wholly distinct botnet – targeting a wholly distinct cluster of websites.”

Spider.io did not disclose which sites received the botnet traffic. But industry executives identified sites owned by San Francisco-based Alphabird, such as ladyshopspot.com, as among the recipients. Advertising space on Alphabird’s sites is sold indirectly through exchanges.

Alphabird described itself as a victim of the scam, noting that it pays for advertising slots on other websites and did not know it had received botnet-generated traffic.

“We buy a lot of media from lots of different people at very high velocity,” said Alex Rowland, Alphabird president. “Anyone that has any significant scale in this marketplace knows that this is a problem in online advertising. Some of these actors are very sophisticated in how they disguise this traffic.”

The issue raises new questions about the controls used by ad technology providers, especially given the ever-changing tactics employed by cyber criminals. Networks of hijacked computers have previously been used to overwhelm a website with traffic, after which botnet operators sometimes demand a ransom to halt the attack. They also frequently seek to collect large numbers of credit card details.

But as online security improves and such attacks become easier to track, botnets are being compared to “victimless” crimes such as insurance fraud – where large numbers of people lose small sums of money, with few of them ever realising they have been ripped off.

Christian Carrillo, a vice-president at DataXu, a digital advertising technology provider, said the fraud could be hard to prosecute even if its perpetrators were tracked down, because of the terms of trade in the online ad business.

---

### Featured on Drudge

Europe's leaders run out of credit in Cyprus

'Slum pope' is sharp political operator

Europe's finance ministers are risking a bank run

New data reveal scale of China abortions

Facebook reveals secrets you haven't shared

### Related articles

Fraudsters exploit web advert algorithms

Former Calpers head charged over fees

BTA entitled to \$2bn from Abylazov

US to ramp up Pacific missile defences

**Printed from:** <http://www.ft.com/cms/s/0/ab60c728-908f-11e2-a456-00144feabdc0.html>

Print a single copy of this article for personal use. Contact us if you wish to print more to distribute to others.

© **THE FINANCIAL TIMES LTD 2013** FT and 'Financial Times' are trademarks of The Financial Times Ltd.